INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 43521-0700	Application Number 10/622,722
	Applicant(s) Hidema TANAKA, T shinobu KANEKO	
	Filing Date July 18, 2003	Group Art Unit TBA

OIPE JC25 JAN 29 2004 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL	REF	DOCUMENT NUMBER		NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation YES	Translation NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

CO		Babbage & Frisch, "On MISTY1 Higher Order Differential Cryptanalysis," 3rd International Conference on Information Security and Cryptology ICISC 2000, Seoul, Korea, December 8-9, 2000 (pp 22-36)
CO		Daemen, Knudsen & Rijmen "The Block Cipher SQUARE", 4th International Workshop FSE '97 on Fast Software Encryption, Haifa, Israel, January 20-22, 1997 (Eli Biham ed.) (pp 149-165)

EXAMINER	/Chinwendu Okoronkwo/	DATE CONSIDERED	01/06/2007

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP Section 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

JAN 29 2007 JC25 PATENT & TRADEMARK OFFICE

Docket Number (Optional)	Application Number
43521-0700	10/622,722
Applicant(s)	
Hidema TANAKA, Toshinobu KANEKO	
Filing Date	**Group Art Unit**
July 18, 2003	TBA

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation YES	Translation NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

CO		Jakobsen & Knudsen "The Interpolation Attack on Block Cipher," FSE-4th International Workshop LNCS 1008
CO		Nyberg, Knudsen, "Provable Security Against Differential Cryptanalysis," Journal of Cryptology, Vol. 8-no. 1

EXAMINER	/Chinwendu Okoronkwo/	DATE CONSIDERED	01/06/2007

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP Section 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

INFORMATION DISCLOSURE CITATION *(Use several sheets if necessary)*	Docket Number (Optional) 43521-0700	Application Number 10/622,722
	Applicant(s) Hidema TANAKA, Toshinobu KANEKO	
	Filing Date July 18, 2003	Group Art Unit TBA

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

OIPE JC25 JUL 29 2004 PATENT & TRADEMARK OFFICE

FOREIGN PATENT DOCUMENTS

	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation YES	Translation NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

CO		Shimoyama, Moriai, Kaneko, "Improving the Higher Order Differential Attack and Cryptanalysis of the KN Cipher," 1997 1st International Workshop on Information Security Workshop LNCS 1396, Tatsunokuchi, Ishikawa, Japan, September 1997 (pp 32-42)
CO		Tanaka, Hisamatsu, Kaneko, "Strength of MISTY1 without FL Function for Higher Order Differential Attack," 13th International (Symposium, Applied Algebra-Algebraic Algorithms and Error-Correcting Codes) 1999, LNCS 1636 (pp 221-231)

EXAMINER /Chinwendu Okoronkwo/	DATE CONSIDERED 01/06/2007

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP Section 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

OIPE SC17D APR 19 2004 PATENT & TRADEMARK OFFICE

Substitute Form PTO-1449 (Modified) U.S. Department of Commerce Patent and Trademark Office	Attorney's Docket No.	Application No.
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))	43521-0700	10/622,722
	Applicant: Tanaka et al.	
	Filing Date: July 18, 2003	Group Art Unit: TBD

U.S. Patent Documents

Examiner Initial	Desig. ID	Patent Number	Issue Date	Patentee	Class	Subclass	Filing Date If Appropriate

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
CO		L. Knudsen, "Truncated and Higher Order Differentials," *Fast Software Encryption: 2nd International Workshop*, Leuven, Belgium (December 14-16, 1994), LNCS 1008, pp. 196-211, Springer-Verlag.
CO		X. Lai, "Higher Order Derivatives and Differentia Cryptanalysis," R[3] Security Engineering AG Ch-8607 Aathal, Switzerland, pp. 1-7; Reprint of pp. 227-233, "Communications and Cryptography," (Ed. R Blahut et al.), Kluwer Academic Publishers (1994).
CO		M. Matsui, "New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis, *Fast Software Encryption: 3rd International Workshop*, Cambridge, UK (February 21-23, 1996), LNCS. 1039, pp. 205-218.
CO		S. Moriai, T. Shimoyama, T. Kaneko, "Higher Order Differential Attack of a CAST Cipher, *Fast Software Encryption: 4th International Workshop*, LNCS 1372, pp. 17-31.

Signature	/Chinwendu Okoronkwo/	Date Considered	01/06/2007

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.